PN - JP11027750 A 19990129

PD - 1999-01-29

PR - JP19970182078 19970708

OPD - 1997-07-08

TI - ACCESS AUTHENTICATION METHOD, CONNECTION CONTROLLER AND COMMUNICATION SYSTEM

IN - YAMADA EIJI;NIINUMA TOKUSHI;TOMOBE YUKIO

PA - KOORASU COMPUTER KK

IC - H04Q7/38 ; H04L9/32 ; H04M3/42

TI - Access authentication method for LAN - involves connecting portable terminal to base apparatus, when input user name and password from portable terminal matches with previously registered name and password

PR - JP19970182078 19970708

PN - JP11027750 A 19990129 DW199915 H04Q7/38 011pp

PA - (CHOR-N) CHORUS COMPUTER KK

IC - H04L9/32 ;H04M3/42 ;H04Q7/38

AB - J11027750 NOVELTY - The telephone number, user name and password, input from a portable terminal (9) are compared with previously registered user name and password corresponding to the telephone number. When the comparison result is in favor, the portable terminal is connected to another base apparatus (4) through a telephone circuit (6) and when not in favor, connection is discarded. DETAILED DESCRIPTION - An independent claim is included for explaining network connection control apparatus.

- USE - For LAN.
- ADVANTAGE - The security of accessing is enhanced by controlling inaccurate access to a network. DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the access authentication apparatus. (4) Receiving-call base apparatus; (6) Telephone circuit network; (9) Portable terminal.
- (Dwg.2/4)

OPD - 1997-07-08

AN - 1999-174046 [15]

PN - JP11027750 A 19990129

PD - 1999-01-29

AP - JP19970182078 19970708

IN - YAMADA EIJI;TOMOBE YUKIO;NIINUMA TOKUSHI

PA - KOORASU COMPUTER KK

TI - ACCESS AUTHENTICATION METHOD, CONNECTION CONTROLLER AND COMMUNICATION SYSTEM

AB - PROBLEM TO BE SOLVED: To enhance security by adopting an authentication method such that the merely the use of a user name and a password does not allow a portable terminal to be connected to a network.

- SOLUTION: When a portable terminal 9 enters a user name, a password and a connection destination telephone number, a communication equipment of a called base station acquires (steps 105, 106) a portable telephone number sent through a telephone exchange network, in response to a caller number notification request. The called base station acquires a caller telephone number from the communication equipment as an authentication key and stores it (steps 107, 108). Upon the receipt of an incoming call, the called base station uses a connection program to acquire a registered user name and a registered password (steps 109, 110). The user name, the password and the caller telephone number that are acquired are compared with those which are registered respectively (step 111), and when they are match, the portable terminal is connected (112) to the network, and when they do not match, the channel is interrupted (113).

I - H04Q7/38 ;H04L9/32 ;H04M3/42

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－27750

(43)公開日　平成11年(1999)１月29日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ	7/26	１０９Ｓ
Ｈ０４Ｌ　9/32		Ｈ０４Ｍ	3/42	Ｔ
Ｈ０４Ｍ　3/42		Ｈ０４Ｌ	9/00	６７３Ｂ
				６７３Ａ

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－182078

(22)出願日　平成９年(1997)７月８日

(71)出願人　597096703
コーラスコンピュータ株式会社
東京都豊島区南池袋１－10－13

(72)発明者　山田　英二
東京都豊島区南池袋１－10－13　コーラスコンピュータ株式会社内

(72)発明者　友部　夕起夫
東京都豊島区南池袋１－10－13　コーラスコンピュータ株式会社内

(72)発明者　新沼　徳士
東京都豊島区南池袋１－10－13　コーラスコンピュータ株式会社内

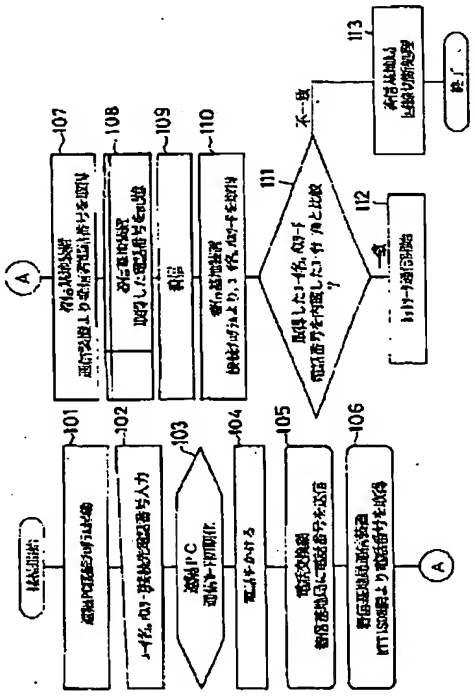
(74)代理人　弁理士　油井　透　（外１名）

(54)【発明の名称】　アクセス認証方法、接続制御装置、及び通信システム

(57)【要約】

【課題】　ユーザ名、パスワードを使うだけでは、携帯端末からネットワークに接続できないようにしてセキュリティを強化する。

【解決手段】　携帯端末９からユーザ名、パスワード、接続先電話番号を入力すると、発信者番号通知要求に応じて電話交換網から送信した携帯電話番号を着信基地局の通信装置が取得する（ステップ１０５、１０６）。着信基地装置は通信装置から発信者電話番号を認証キーとして取得し記憶する（ステップ１０７、１０８）。着信基地装置は着信があると接続プログラムにより、登録したユーザ名、パスワードを取得する（ステップ１０９、１１０）。取得したユーザ名、パスワード、発信者電話番号を、登録したユーザ名、パスワード、携帯電話番号とそれぞれ比較して（ステップ１１０）、一致したとき携帯端末をネットワークに接続し（ステップ１１２）、不一致のときは回線を切断する（ステップ１１３）。



【特許請求の範囲】
【請求項1】複数のアクセス装置が通信可能に接続される被アクセス装置のためのアクセス認証方法において、認証キーとして、上記アクセス装置側からのアクセス要求があったとき、被アクセス装置側に自動的に送られる上記アクセス装置を特定するための情報を使用したことを特徴とするアクセス認証方法。
【請求項2】上記認証キーとして、ユーザ名、パスワードに加えて上記アクセス装置特定情報を被アクセス装置側に登録し、これらの登録情報であるユーザ名、パスワードおよびアクセス装置特定情報と、被アクセス装置側に送られてくるユーザ名、パスワード、およびアクセス装置特定情報とが全て一致したときだけ、アクセス装置を上記被アクセス装置に接続するようにしたことを特徴とする請求項1に記載のアクセス認証方法。
【請求項3】上記アクセス装置特定情報が、アクセス装置の電話番号である請求項1または2に記載のアクセス認証方法。
【請求項4】端末からのアクセス要求がネットワークにあったとき、発信者番号通知要求に応じて上記端末とネットワークとの間に介在する電話交換網から上記ネットワーク側に上記端末の発信者電話番号を通知するサービス機能を利用したアクセス認証方法において、
上記ネットワーク側に上記端末を認識して接続するために設けられた接続制御装置に、上記ネットワークへのアクセス要求を認証するためのユーザ名、パスワードおよび上記端末の電話番号を予め登録し、
上記端末からの上記ネットワークへのアクセス要求により、上記発信者番号通知要求に応じて上記電話交換網から端末の発信者電話番号を、端末から送信される上記ユーザ名、パスワードとともにアクセス要求先の上記接続制御装置に送信し、
送信されてきた上記ユーザ名、パスワード、及び端末発信者電話番号を、上記接続制御装置に登録したユーザ名、パスワード、端末電話番号とそれぞれ比較して、いずれもが一致したときは上記端末を上記ネットワークに接続し、不一致のときは回線を切断するようにしたことを特徴とするアクセス認証方法。
【請求項5】複数のアクセス装置と被アクセス装置とが交換網を介して通信可能に接続される通信システムの被アクセス装置側に設けられるものであって、
前記アクセス装置からアクセス要求が発生すると、このアクセス要求が発生したアクセス装置を特定するために上記交換網から送られてくるアクセス装置特定情報、および前記アクセス装置から送られてくるユーザ名、パスワードに基づいて前記アクセス装置を前記被アクセス装置に接続してよいか否かを判定する判定手段と、
この判定手段の判定結果に基づいて被アクセス装置に対する当該アクセス装置の接続を制御する接続制御手段とを備えた接続制御装置。
【請求項6】複数の端末とネットワークとが電話交換網を介して通信可能に接続される通信システムのネットワーク側に設けられるものであって、
ユーザ名、パスワードに加えて、さらに端末の電話番号を登録する記憶手段と、
この記憶手段に登録されたユーザ名、パスワード及び端末電話番号と、上記端末からアクセス要求が発生すると、このアクセス要求が発生した端末を特定するために上記電話交換網から送られてくる端末の発信者電話番号、および上記端末から送られてくるユーザ名、パスワードとをそれぞれ比較して、これらが全て一致したとき上記端末を上記ネットワークに接続してよいと判定し、一部でも不一致のとき上記端末と上記ネットワークとの回線を切断してよいと判定する判定手段と、
この判定手段の一致判定に基づいて被アクセス装置に当該アクセス装置を接続し、不一致判定に基づいて回線を切断する接続制御手段とを備えた接続制御装置。
【請求項7】請求項6に記載の接続制御装置を備え、複数の端末とネットワークとが電話交換網を介して通信可能に接続される通信システムにおいて、
上記電話交換網が、上記端末から上記ネットワークにアクセス要求があったとき、発信者番号通知要求に応じて上記接続制御装置に発信者電話番号を通知するサービス機能を有することを特徴とする通信システム。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は通信システムのアクセス認証方法、接続制御装置、及び通信システムに係り、特に被アクセス側とアクセス側が1：Nの関係となる通信システムのセキュリティを向上するのに好適なものに関する。
【0002】
【従来の技術】ネットワーク例えばオフィスLANないし社内LANに対する外部アクセスのセキュリティを確保するためには、アクセスしてくるユーザを認証する必要がある。その認証方法として従来次のようなものがあった。
【0003】(1) PAP(Password Authentication Protocol)認証方式
インターネットプロバイダ（通信網接続業者）やモバイルコンピューティングに使用されている着信基地装置、例えばリモートアクセスサーバ（RAS）で行なわれる認証方式であり、ユーザ登録したユーザ名、パスワードと、ユーザ端末例えば遠隔PCから送られてきたユーザ名、パスワードとを比較することによって利用者の確認を行なっている。ユーザ名は、パスワードをキーとして圧縮する方式もある（CHAP(Change code Authentication Protocol）認証方式）。
【0004】(2) ICカードセキュリティ方式
遠隔PC（遠隔パーソナルコンピュータ）にCPUを搭

載した認証ＩＣカードを接続し、そのＩＣカードによって本人か否かを認証する方式であり、通常、ユーザ名、パスワードと併用される。ＩＣカードをもっていれば本人と認められるので、完璧なセキュリティが期待できるといわれている。

【０００５】(3) ワンタイムパスワード
遠隔ＰＣのユーザにパスワード発生装置を配布し、そのパスワードを入力する。ＲＡＳには、そのパスワード発生装置の固有コードを登録し、一定の計算式によってパスワードを解読する。

【０００６】
【発明が解決しようとする課題】しかしながら、上述した従来の認証方式には次のような欠点があった。

【０００７】(1) ＰＡＰ認証方式は、ユーザ端末を選ばないため、ユーザ名、パスワードが漏洩したり、他人に盗まれたりした場合には、本人以外でもどんな端末からでも簡単に接続ができてしまうために、不正な接続を有効に防止できない。

【０００８】(2) ＩＣカード方式は、完璧なセキュリティを望むばあいにはふさわしいが、遠隔ＰＣにＩＣカードを搭載するための拡張スロットを必要とする上、端末側に何らかのプログラムを追加する必要があり、しかもプログラムやＯＳによる機種依存がある。また、ＩＣカードを紛失すると本人であっても接続できなくなる。

【０００９】(3) ワンタイムパスワード方式は、遠隔ＰＣの利用者にパスワード発生装置を配布する必要があるうえ、計算式は製造元によって異なり、しかも端末側は何らかのプログラムを通過する必要があり、プログラムやＯＳによる機種依存がある。

【００１０】このような従来の認証方式では、３２ｋｂｐｓ高速ＰＨＳのような高速通信可能な携帯端末の出現により、爆発的な増加が予想されるモバイルコンピューティングのセキュリティに十分対応できない。

【００１１】本発明の目的は、複数のアクセス装置が通信可能に接続される被アクセス装置のためのアクセス認証において、上述した従来技術の問題点を解消して、認証キーに端末認証機能をもたせることによって端末自体の認証を行い、もって機種依存がなく、簡単にセキュリティを高めることができるアクセス認証方法、接続制御装置、及び通信システムを提供することにある。

【００１２】
【課題を解決するための手段】請求項１に記載の発明は、複数のアクセス装置が通信可能に接続される被アクセス装置のためのアクセス認証方法において、認証キーとして、上記アクセス装置側からのアクセス要求があったとき、被アクセス装置側に自動的に送られる上記アクセス装置を特定するための情報を使用したものである。

【００１３】被アクセス側で認証する認証キーにアクセス装置の特定情報を使用すると、被アクセス装置側でアクセス装置自体を特定することができるので、通信可能に接続される複数のアクセス装置が不特定のアクセス装置であっても、アクセス装置を盗まれない限り、被アクセス装置への不正なアクセスを防止できるので、アクセスユーザ面からのセキュリティに対してアクセス装置面からのセキュリティを確保することができる。

【００１４】請求項２に記載の発明は、上記認証キーとして、ユーザ名、パスワードに加えて上記アクセス装置特定情報を被アクセス装置側に登録し、これらの登録情報であるユーザ名、パスワードおよびアクセス装置特定情報と、被アクセス装置側に送られてくるユーザ名、パスワード、およびアクセス装置特定情報とが全て一致したときだけ、アクセス装置を上記被アクセス装置に接続するようにしたものである。

【００１５】ユーザ名、パスワードに加えてアクセス装置特定情報を認証することにより、アクセスユーザとアクセス装置との両面からアクセス要求を認証できるようにしたので、被アクセス装置のセキュリティ機能をさらに強化することができる。

【００１６】請求項３に記載の発明は、上記アクセス装置特定情報を、アクセス装置の電話番号としたものである。

【００１７】アクセス装置の発信者電話番号は、一般ユーザがこの番号を変更して、不正に使用することは事実上不可能なことから、セキュリティを一層高めることができる。

【００１８】請求項４に記載の発明は、端末からのアクセス要求がネットワークにあったとき、発信者番号通知要求に応じて上記端末とネットワークとの間に介在する電話交換網から上記ネットワーク側に上記端末の発信者電話番号を通知するサービス機能を利用したアクセス認証方法において、上記ネットワーク側に上記端末を認識して接続するために設けられた接続制御装置に、上記ネットワークへのアクセス要求を認証するためのユーザ名、パスワードおよび上記端末の電話番号を予め登録し、上記端末からの上記ネットワークへのアクセス要求により、上記発信者番号通知要求に応じて上記電話交換網から端末の発信者電話番号を、端末から送信される上記ユーザ名、パスワードとともにアクセス要求先の上記接続制御装置に送信し、送信されてきた上記ユーザ名、パスワード、及び端末発信者電話番号を、上記接続制御装置に登録したユーザ名、パスワード、端末電話番号とそれぞれ比較して、いずれもが一致したときは上記端末を上記ネットワークに接続し、不一致のときは回線を切断するようにしたものである。

【００１９】電話交換網が有する発信者番号通知サービスを利用するようにしたので、通信システムや通信ソフトに変更を加えることなく、認証システムを構築できる。また、ユーザ名、パスワードを他人に盗まれた場合であっても、本人のユーザ端末以外からは接続ができないために、不正なネットワーク接続を防止できる。ま

た、端末だけを盗まれた場合にも、ユーザ名、パスワードがわからなければ接続できない。さらにユーザ名、パスワード、及び端末を全て盗まれた場合でも、接続制御装置のユーザ登録を無効にするだけで簡単、かつ確実に不正接続を予防することができる。

【００２０】請求項５に記載の発明は、複数のアクセス装置と被アクセス装置とが交換網を介して通信可能に接続される通信システムの被アクセス装置側に設けられるものであって、前記アクセス装置からアクセス要求が発生すると、このアクセス要求が発生したアクセス装置を特定するために上記交換網から送られてくるアクセス装置特定情報、および前記アクセス装置から送られてくるユーザ名、パスワードに基づいて前記アクセス装置を前記被アクセス装置に接続してよいか否かを判定する判定手段と、この判定手段の判定結果に基づいて被アクセス装置に対する当該アクセス装置の接続を制御する接続制御手段とを備えた接続制御装置である。

【００２１】通信システムの被アクセス装置側に、判定手段と接続制御手段とを備えた接続制御装置を設けるだけの簡単な構造で、通信可能に接続される複数のアクセス装置が不特定のアクセス装置であっても、ユーザ名及びパスワードからユーザを認証するとともに、アクセス要求のあったアクセス装置特定情報からアクセス装置を認証して、当該アクセス装置の接続を制御するようにしたので、ユーザ及びアクセス装置の両面からセキュリティを確保でき、被アクセス装置への不正なアクセスを有効に防止できる。

【００２２】請求項６に記載の発明は、複数の端末とネットワークとが電話交換網を介して通信可能に接続される通信システムのネットワーク側に設けられるものであって、ユーザ名、パスワードに加えて、さらに端末の電話番号を登録する記憶手段と、この記憶手段に登録されたユーザ名、パスワード及び端末電話番号と、上記端末からアクセス要求が発生すると、このアクセス要求が発生した端末を特定するために上記電話交換網から送られてくる端末の発信者電話番号、および上記端末から送られてくるユーザ名、パスワードとをそれぞれ比較して、これらが全て一致したとき上記端末を上記ネットワークに接続してよいと判定し、一部でも不一致のとき上記端末と上記ネットワークとの回線を切断してよいと判定する判定手段と、この判定手段の一致判定に基づいて被アクセス装置に当該アクセス装置を接続し、不一致判定に基づいて回線を切断する接続制御手段とを備えた接続制御装置である。

【００２３】接続制御装置に、ユーザ名、パスワード、端末電話番号を登録する記憶手段を設けたので、ユーザ登録及び登録抹消が簡単で、仮にユーザ名、パスワード、端末が盗まれても、ユーザ登録を抹消すれば、不正なアクセスを予防できる。

【００２４】請求項７に記載の発明は、請求項６に記載の接続制御装置を備え、複数の端末とネットワークとが電話交換網を介して通信可能に接続される通信システムにおいて、上記電話交換網が、上記端末から上記ネットワークにアクセス要求があったとき、発信者番号通知要求に応じて上記接続制御装置に発信者電話番号を通知するサービス機能を有する通信システムである。

【００２５】電話交換網が有する発信者番号通知サービスを利用するようにしたので、通信システムや通信ソフトに変更を加えることなく、認証システムを容易に構築できる。

【００２６】

【発明の実施の形態】以下に本発明の実施の形態を説明する。ＮＴＴが行なっている通信サービスの一つに、発信者番号通知サービスがある。これは発信者の電話番号が、着信者の電話機などに電話に出る前に通知されるサービスで、その仕組みは図４に示すようになっている。着信側がこのサービスを受けている場合、ＰＨＳなどの携帯端末３５の電話番号は携帯端末３５から送信されるものではなく、電話番号の管理をおこなっているＮＴＴの電話交換網３３から着信側に送信される。携帯端末３５から携帯端末機中継基地３４に向けて接続先にアクセス要求すると、携帯端末３５から携帯端末固有のコードが自動的に送信されるとともに発信者電話番号通知要求が出される。これらの情報を受信した電話交換網３３は、その電話番号データベースから電話機固有コードに関連づけられた発信者電話番号を割出す。また、接続先の電話番号につながるように回線接続交換を行なって、電話回線網３２を着信電話機３１に接続し、発信者電話番号を送信し、着信電話機３１の表示装置に発信者電話番号を表示するサービスである。

【００２７】このサービスの主な用途は、発信側に返信するコールバックを行なったり、必要な通話以外着信しないとか、識別着信に使用したりすることである。ＮＴＴに依頼すれば、ＩＳＤＮ回線に上記発信者番号通知機能を設定することができる。ＮＴＴおよび通信網接続業者はこの発信者番号通知サービスを要求により停止、変更することができる。携帯端末３５の電話番号は携帯端末３５から送信されるものではなく、電話交換網３３から送信されるので、携帯端末３５のユーザは発信者電話番号を故意に変更することはできない。

【００２８】本実施の形態は、上述した発信者番号通知サービス機能をセキュリティの一部に利用したものであり、ターミナルアダプタ（ＴＡ）などの通信装置に発信者電話番号を受け取る機能をもたせるとともに、ＴＡに接続されるリモートアクセスサーバなどの着信基地装置に発信者電話番号を認証できる機能を追加したものである。

【００２９】図２に本発明のアクセス認証方法を実施するための通信システムの実施形態を示す。被アクセス装置としての着信基地局１はネットワーク１２を構成す

る。そのネットワークケーブル２には、遠隔ネットワークサーバ３や、図示しないデータベース、複数のクライアントＰＣ（パーソナルコンピュータ）、ネットワーク１２にＰＨＳなどのアクセス装置である携帯端末９を接続するための着信基地装置４、ネットワーク１２を電話回線網６に接続するための通信装置５などが接続される。上記着信基地装置４および通信装置５で接続制御装置を構成する。

【００３０】上記ネットワーク１２は、オフィスＬＡＮ、ルータで相互接続されたＬＡＮ、ＢＢＳ（ＢｕｌｌｅｔｉｎＢｏｒｄＳｙｓｔｅｍ）などの、不特定多数からのアクセスが可能な情報通信網（１：Ｎ）から構成され、有線ネットワーク、無線ネットワーク、衛星ネットワーク、ファイバ光ケーブルネットワーク、同軸ケーブルネットワークのいずれでもよい。

【００３１】上記着信基地装置４は、例えばリモートアクセスサーバ（ＲＡＳ）と呼ばれるもので構成され、オフィスクライアントとしてのネットワーク１２に、モバイルクライアント側遠隔ＰＣ１１に接続する携帯端末をあたかもＮＩＣ（ネットワークインタフェースカード）として認識させるための環境を提供するモバイルコンピューティングのためのサーバである。特に、本実施の形態では、ユーザ名、パスワードに加えて発信者電話番号を認証できる機能を搭載している。

【００３２】通信装置５は、ネットワーク１２と電話回線網６とをつなぐモデム、遠隔ＰＣをＩＳＤＮ回線に接続するＴＡ、携帯電話対応のＴＡ、ＰＩＡＦＳ対応ＴＡ（ＴＡＰ）などから構成され、前述した発信者番号通知を電話回線網６から受け取る機能を持っている。特にＴＡＰはモバイルクライアントからの通信も通常のＴＡからの通信も自動的に識別して接続することができる。なお、ＰＩＡＦＳ（ＰＨＳＩｎｔｅｒｎｅｔＡｃｃｅｓｓＦｏｒｕｍＳｔａｎｄａｒｄ）とは、ＰＨＳ高速無線通信の標準プロトコルである。

【００３３】このように構成された着信基地局１は、電話回線網６、ＮＴＴ電話番号データベースを有する電話交換網７、ＰＨＳ．携帯電話などの携帯端末中継基地８を介して不特定の携帯端末９と通信可能に結合されるようになっている。携帯端末９は、データ通信を行うための通信カード１０を介して遠隔ＰＣ１１に接続される。ここで上記電話回線網６は、一般公衆回線、ＩＳＤＮ回線もしくは携帯電話、ＰＨＳなどの電波網、さらにはコンピュータネットワークでもよい。また、携帯端末９は、モデム、ターミナルアダプタ、もしくはＰＨＳ電話機、携帯電話機、無線機などであり、遠隔ＰＣはモバイルコンピュータやＰＤＡ（個人用情報機器）などで構成される。ＰＤＡには、携帯端末９、通信カード１０、遠隔ＰＣ１１を一体化したものもある。

【００３４】図３は発信者電話番号を認証できる機能を搭載した上記着信基地装置４のブロック図である。その構成を動作とともに説明する。

【００３５】通信装置５からの発信者電話番号を含むアクセス情報はシリアルインタフェースコネクタ２５を通じて、シリアルインタフェースコントローラで構成される通信制御装置２４が受信し、全体を制御する判定手段としての中央制御装置（ＣＰＵ）２３に渡される。中央制御装置２３は、基本ＯＳの制御を行うとともに、通信装置５から送られてくる情報のユーザ名、パスワード、発信者電話番号と、予め登録したユーザ名、パスワード及び発信者電話番号とを比較演算処理し、その処理結果に応じて、イーサネットコントローラなどからなる接続制御手段としてのＬＡＮシステム制御装置２２を制御し、イーサネットインタフェースコネクタ２１を介して携帯端末９をＬＡＮに接続するか、または着信基地局１との回線を切断する。

【００３６】中央制御装置２３に接続される揮発性記憶装置２６は、ＲＡＭから構成されたワークメモリであり、中央制御装置２３の演算処理時に一時的にデータを格納したり、送受信バッファとして機能する。また通信装置５から送られてくるユーザ名、パスワード及び発信者電話番号を中央制御装置２３を介して格納する。格納したユーザ名、パスワード及び電話番号は、中央制御装置２３で行なわれる認証のための比較演算処理のとき、揮発性記憶装置２６から読み出される。不揮発性記憶装置２７はユーザメモリであり、認証キーとしてのユーザ情報、すなわちネットワーク１２へのアクセス要求が許容されるユーザ名、パスワード、及びユーザ携帯端末の電話番号を登録する。これらの情報を登録する不揮発性記憶装置２７としては、たとえば書換えが可能なＥＰＲＯＭが好ましい。

【００３７】このユーザ情報も、中央制御装置２３で行なわれる認証のための比較演算処理のとき、不揮発性記憶装置２７から読み出される。不揮発性記憶装置２７にはさらに駆動プログラム、制御基本設定データが格納される。読出し専用記憶装置２８はシステムＲＯＭであり、中央制御装置２３を制御する基本ＯＳ、および非常時の作動プログラムが格納される。着信基地装置４の各部への電力供給は外部電源２９から電源回路３０を介して供給される。なお外部電源２９は内蔵バッテリであってもよい、また、図示例では通信制御装置（シリアルインタフェースコントローラ）２４をシリアルインタフェースコネクタ２５と中央制御装置２３との間に介在するようにしたが、直接中央制御装置２３に通信装置５を接続する場合もある。

【００３８】このように着信基地装置４は、認証キーとして携帯端末の電話番号も不揮発性記憶装置２７に登録することにより、発信者番号通知要求により電話交換網７から送られてくる発信者電話番号の認証も行なえるようにしている。

【００３９】図１に、上記構成に基づいた認証方法のフ

ローを示す。遠隔ＰＣ１１にＰＨＳなどの携帯端末９を接続した通信カード１０を装着したうえで遠隔ＰＣ１１の電源を入れ、アクセス要求するための接続プログラムを起動する（ステップ１０１）。遠隔ＰＣ１１の入力部からユーザ名、パスワード及び接続先のネットワーク１２の電話番号を入力する（ステップ１０２）。

【００４０】遠隔ＰＣ１１は通信カード１０を初期化し（ステップ１０３）、携帯端末９を介して接続先に電話をかける（ステップ１０４）。携帯端末中継基地８を介して携帯端末固有コードを含むアクセス情報を受けた電話交換網７は、そのＮＴＴ電話番号データベースから携帯端末固有コードに基づいて当該アクセスしてきた発信者電話番号を割出し、割出した発信者電話番号を電話回線網６を介して自動的に着信基地局１に送信する（ステップ１０５）。着信基地局１側の通信装置５は電話回線網６より発信者電話番号を取得する（ステップ１０６）。

【００４１】着信基地装置４は、通信装置５からの上記発信者電話番号を取得し（ステップ１０７）、取得した発信者電話番号を揮発性記憶装置２６に記憶する（ステップ１０８）。着信基地装置４は着信後、接続プログラムによって携帯端末９から送られてくるユーザ名、パスワードを取得する（ステップ１０９、１１０）。そのうえで、携帯端末９から取得したユーザ名、パスワード、および揮発性記憶装置２６に格納した発信者電話番号を、不揮発性記憶装置２７にユーザ登録したユーザ名、パスワード及びユーザ電話番号と比較する（ステップ１１１）。これらの全てが一致したらネットワーク通信を開始し（ステップ１１２）、不一致のときは不正ユーザからのアクセス要求ないしアクセス要求情報に誤りがあるとして着信基地局１の回線切断処理をおこなう（ステップ１１３）。

【００４２】上述したように本実施の形態は、ＮＴＴの電話通信網で制定される固有の端末電話番号を着信基地局側に登録しておくもので、これをセキュリティのキーに適用したものであり、電話番号は、各回線毎の固有の番号で、基本的に重複することはなく、一般の端末ユーザがこの番号を変更して、不正に使用することは事実上不可能である。したがって、電話番号は各利用者の固有の認証キーとして機能し、この認証キーにユーザ名、パスワードも加わるので、これらが全て着信基地局側の登録内容と一致しない限り接続を許可しないため、セキュリティが飛躍的に向上する。

【００４３】また、ユーザを特定するユーザ名、パスワードに加えて、携帯端末を特定する発信者電話番号も認証するようにしたので、仮にユーザ名、パスワードを他人に盗まれた場合であっても、携帯端末電話番号が登録された正規の携帯端末以外からではネットワーク１２に接続ができないために、不正なネットワーク接続を有効に防止できる。携帯端末だけを盗まれた場合には、ユーザ名、パスワードがわからなければ接続できないので、完璧なセキュリティを実現できる。

【００４４】また、携帯端末９や電話交換網７のシステム、さらに着信基地局１側のネットワーク１２には全く手を加えずに、既存の通信装置５を発信者番号通知サービス対応にするとともに、同じく既存の着信基地装置４に発信者電話番号認証機能を付加するという僅かな変更を加えるだけですむので、従来考えられているＩＣカード方式やワンタイムパスワード方式を採用する場合に比して、システム構成をきわめて簡単に構築でき、機種依存も、認証対象の紛失のおそれもない。特に、発信者番号通知サービスに対応した通信装置は既に実用化されており、またユーザ名、パスワードで認証を行ってモバイルコンピュータをＬＡＮに接続する着信基地装置も実用化されている。従って、着信基地装置のみに僅かな変更を加えるだけで上記電話番号の認証を行うことができるようになるので、実用化がきわめて容易である。

【００４５】また、新たに加える認証キーとしての発信者電話番号は、発信者番号通知サービスを利用しているため、ユーザ携帯端末９から発信するユーザ名、パスワードと異なり、電話交換網７から送信されるので、ユーザが送信する必要がなく、ユーザに負担をかけない。また、この発信者電話番号はユーザが送信できないことから却ってユーザ側で不正な操作をすることができず、電話番号認証がやぶられることがなく、発信者電話番号認証を加えることによりセキュリティを大幅に強化できる。このことは、特に不特定多数からのアクセスを前提とするＬＡＮシステムなどにとっては重要である。

【００４６】また、上記実施の形態では、ネットワークに遠隔ＰＣを認識させ、かつ認証する機能を専用のハードウェア（着信基地装置）によって実行するようにしたが、イーサネット、モデム制御装置、メモリなどを備えたパソコンやワークステーションなどを使いソフトウェアによって行うようにしてもよい。また、アクセス装置である携帯端末としては、ＰＨＳ以外に、携帯電話やアナログ電話、ディジタル電話、衛星通信電話などでも、通信機器が対応すれば適用できる。さらに、無線の携帯端末に限定されず、有線のアナログ電話であってもよい。またネットワークは遠隔通信ネットワークに限定されず、隣接するＬＡＮ間でもよい。

【００４７】

【実施例】

(1) リモートアクセスサーバ（ＲＡＳ）の発信者通知認証時の基本データ仕様

受信電話番号	文字形式２５文字以上（ＡＳＣＩＩ文字形式） ハイフンなどの記号を含まない
ユーザ名	８文字以上、半角文字（ＡＳＣＩＩ文字形式）

大文字、小文字の区別を行う
パスワード　８文字以上、半角文字（ＡＳＣＩＩ文字形式）
大文字、小文字の区別を行う
判定方法　ユーザテーブル（登録データ）と上記データは全て文字列が一致
したときにアクセス成功

(2) 通信装置のハード的な対応仕様
ＮＴＴの定める発信者番号通知機能を利用して、回線接続時に端末側の発信者電話番号を受信できること（回線接続の際にＲＩＮＧ文字列に続き、電話番号を取得できる通信機能）。

【００４８】例：RING0000000000
シリアルポートまたは専用バスに接続し、着信基地装置に発信者電話番号を送信できること。

【００４９】(3) アクセス装置（携帯端末）のハード的な対応仕様
ＮＴＴの定める発信者通知機能を利用して、回線接続時に発信側の発信者番号通知要求を送信できること。

【００５０】シリアルポートまたは専用バスに接続し、電話交換網にアクセス装置の固有コードを送信できること。

【００５１】社内ＬＡＮと接続されたＲＡＳに社員のユーザ名、パスワード及び社員が携帯するＰＨＳ（ＰＩＡＦＳ対応）の電話番号を登録する。ＰＩＡＦＳ対応の通信カードを使ってＰＨＳから発信者番号通知要求により、発信者番号通知機能に対応した通信装置で、世界に１つしかないＰＨＳの電話番号である発信者番号（RING0000000000）を取得してＲＡＳで認証する。認証方式はＰＰＰ（Point to Point Protocol ）である。ＰＨＳからアクセス要求があったとき、社内ＬＡＮと接続されたＲＡＳに電話番号を送信して登録されているかを確認し、そのＰＨＳを携帯する社員にユーザ名とパスワードを請求した後で、再度、電話番号とパスワードが一致するかを確認して接続許可をする。これにより爆発的な増加が予想されるモバイルコンピューティングのセキュリティに十分対応できる。なお、全て標準機能を利用するため、利用料金がかからないというメリットもある。

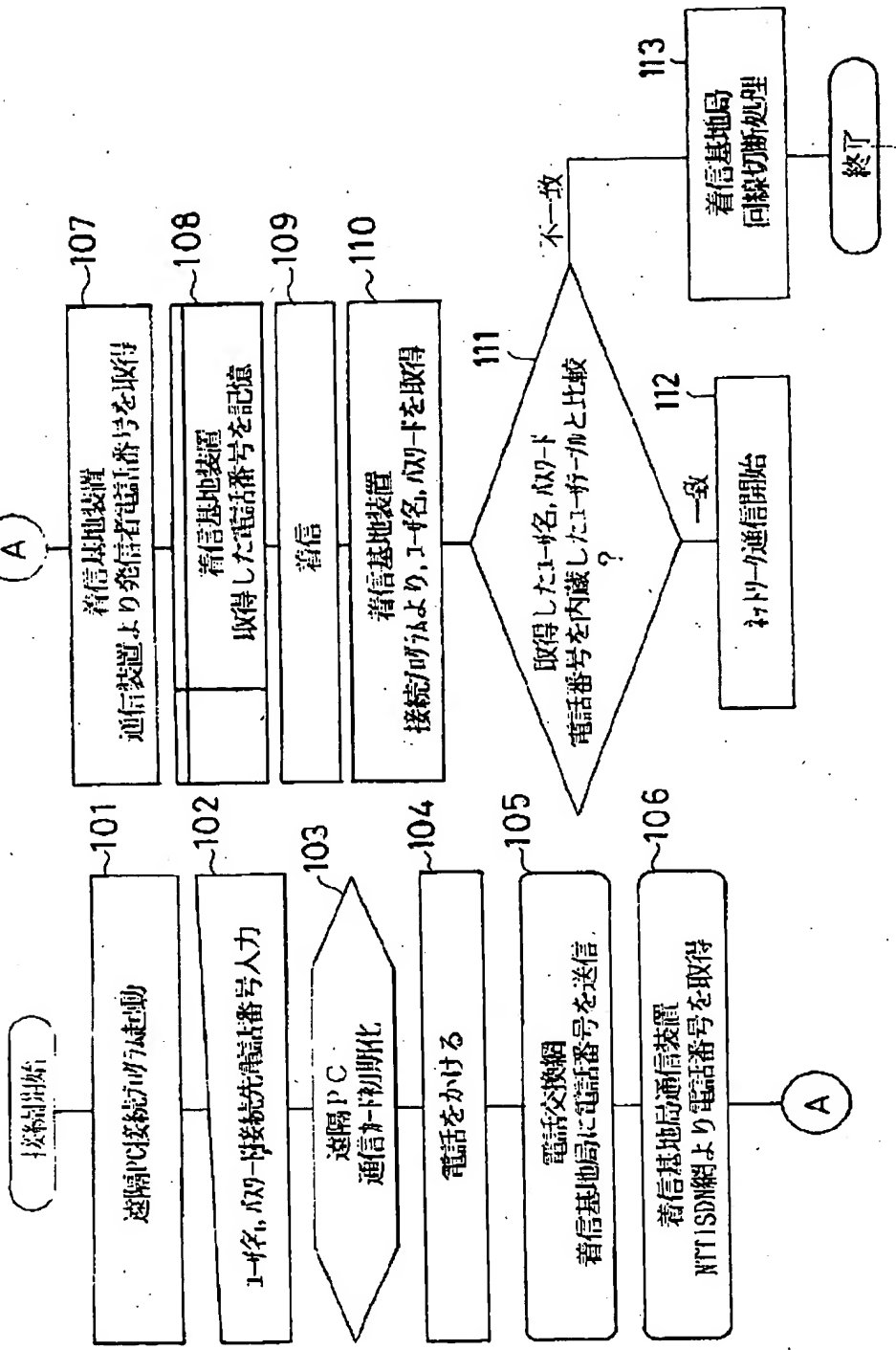
【００５２】【発明の効果】本発明によれば、アクセス装置からのアクセス要求に関連づけられてネットワーク側に自動的に送られるアクセス装置を特定するためのアクセス特定情報を認証キーに使用したので、特定のアクセス装置からのアクセスのみが許容され、ネットワークへの不正なアクセスを規制できるので、不特定のアクセス装置からのアクセスが可能なネットワークなどの被アクセス装置のセキュリティを高めることができる。

【００５３】特に、アクセス特定情報として、アクセス装置から発信するようなユーザ名やパスワードとは異なり、電話交換網から発信する発信者電話番号を利用すると、発信者電話番号はユーザが不正に使用できないので、高度なセキュリティシステムを既存システムをいじらないで簡単に構築できる。

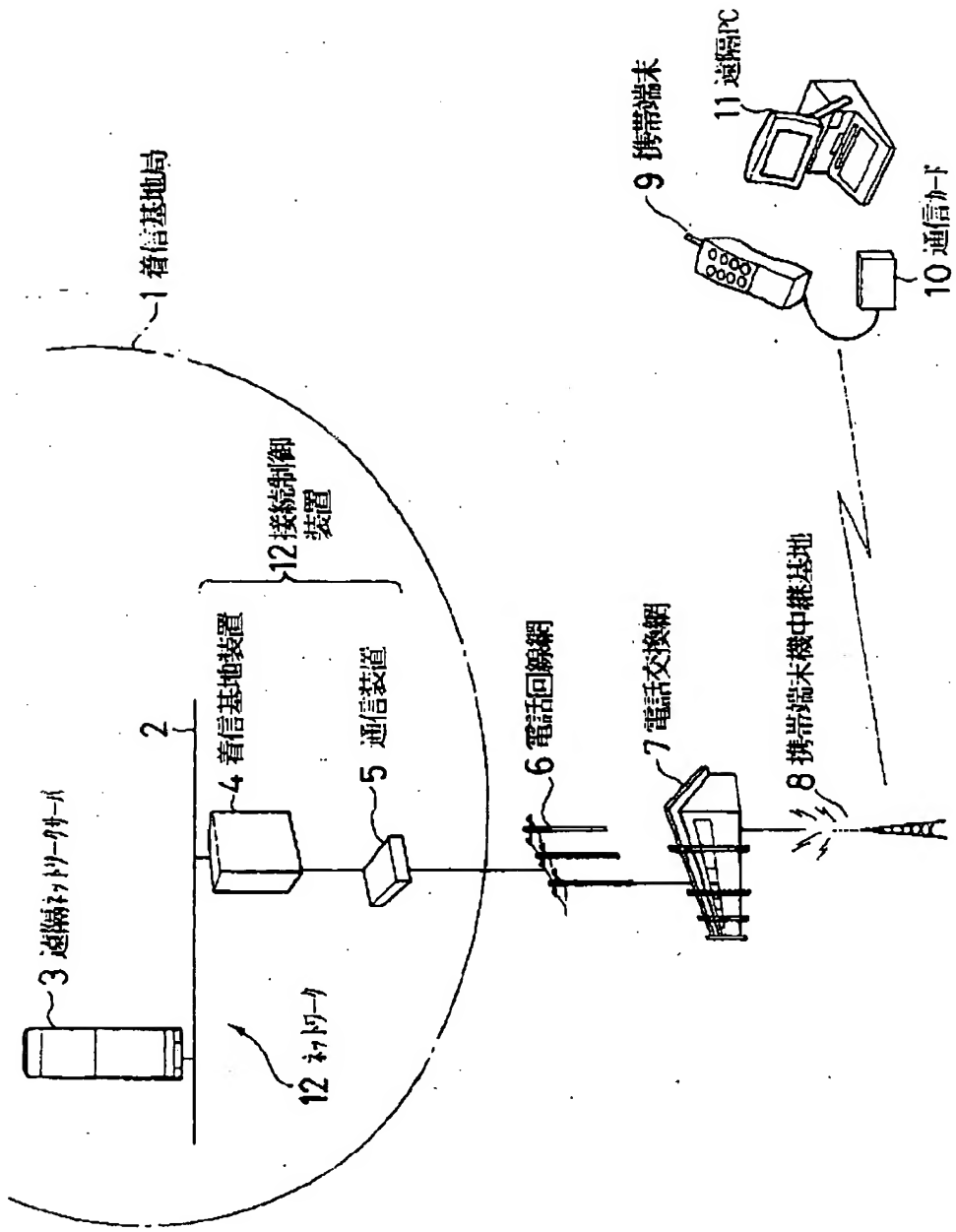
【図面の簡単な説明】
【図１】実施の形態を示す認証方式の流れを示すフローチャートである。
【図２】実施形態の認証装置の構成図である。
【図３】認証装置を構成する実施形態の着信基地装置のブロック図である。
【図４】発信者番号通知サービスの仕組みを示す説明図。

【符号の説明】
１　着信基地局
２　ネットワークケーブル
４　着信基地装置
５　通信装置
６　電話回線網
７　電話交換網
９　携帯端末
１１　遠隔ＰＣ
１２　ネットワーク

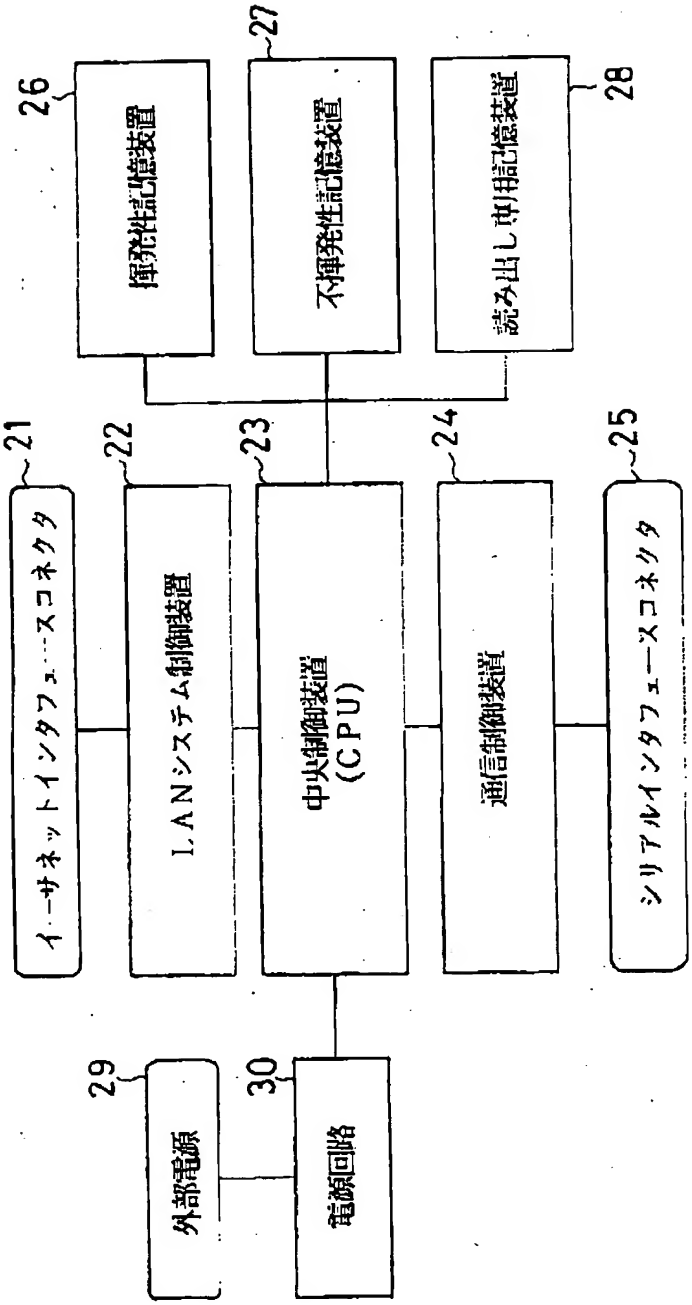
【図1】


接続開始
101
遠隔PC接続方法起動
102
ユーザ名，パスワード接続先電話番号入力
103
遠隔PC
通信カード初期化
104
電話をかける
105
電話交換網
着信基地局に電話番号を送信
106
着信基地局通信装置
NTT ISDN網より電話番号を取得
A
A
107
着信基地装置
通信装置より発信者電話番号を取得
108
着信基地装置
取得した電話番号を記憶
109
着信
110
着信基地装置
接続方法より，ユーザ名，パスワードを取得
111
取得したユーザ名，パスワード
電話番号を内蔵したユーザテーブルと比較
?
一致
112
ネットワーク通信開始
不一致
113
着信基地局
回線切断処理
終了

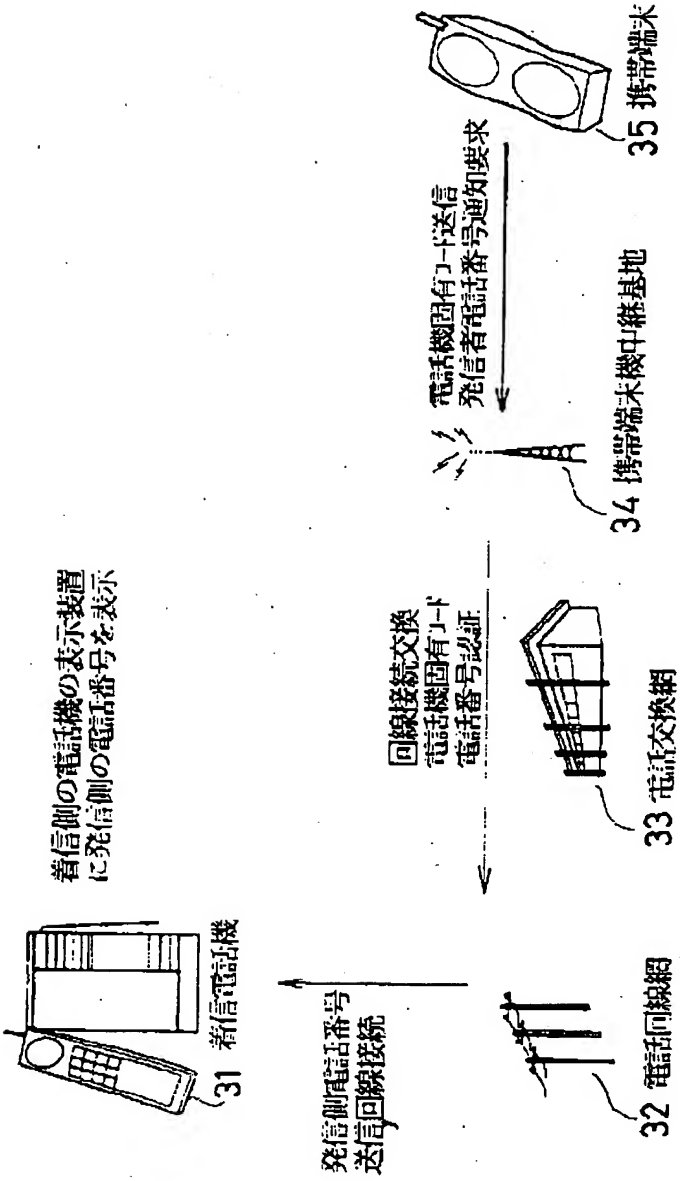
【図2】


1 着信基地局
2
3 遠隔ネットワークサーバ
4 着信基地装置
5 通信装置
6 電話回線網
7 電話交換網
8 携帯端末機中継基地
9 携帯端末
10 通信カード
11 遠隔PC
12 ネットワーク
12 接続制御装置

【図3】


揮発性記憶装置
26
不揮発性記憶装置
27
読み出し専用記憶装置
28
イーサネットインタフェースコネクタ
21
LANシステム制御装置
22
中央制御装置
(CPU)
23
通信制御装置
24
シリアルインタフェースコネクタ
25
外部電源
29
電源回路
30

【図4】


着信側の電話機の表示装置
に発信側の電話番号を表示
31 着信電話機
発信側電話番号
送信回線接続
32 電話回線網
回線接続交換
電話機固有ｺｰﾄﾞ
電話番号認証
33 電話交換網
34 携帯端末機中継基地
電話機固有ｺｰﾄﾞ送信
発信者電話番号通知要求
35 携帯端末